IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Trends And Challenges In Cloud Computing Security

1st Author : **Miss. Sanika Machchindra Hinge**, 2nd Author: **Miss.Ashwini Atul Pansare,**

JCEI's Jaihind Institute of Management and Research (MCA)

3rd Author **: Prof.Dnyaneshwar Balu Lokhande(Research Guide),**4th Author**:Prof.Shubhangi Pratik Bombale(Research Guide)**

Abstract: Cloud computing allows organizations to manage data and run applications on remote infrastructures offered by providers like AWS, Microsoft Azure, and Google Cloud. These platforms deliver numerous advantages—including cost savings, high availability, and global accessibility. However, alongside these benefits, cloud environments face several complex security concerns such as unauthorized access, misconfigured services, data leaks, and vulnerabilities created by shared resources.

Traditional perimeter-based security models are unsuitable for dynamic cloud ecosystems. Modern architectures demand continuous user validation, automated policy enforcement, and AI-powered monitoring to detect threats in real time. This paper examines current trends that influence cloud security and identifies the most frequent challenges faced by organizations today.

Index Terms **-** Cloud Security, Zero Trust, DevSecOps, Multi-Cloud, CNAPP, AI Security, Misconfiguration.

I. INTRODUCTION

Cloud computing enables organizations to store, process, and manage data over remote infrastructure provided by AWS, Azure, and Google Cloud. While offering cost efficiency and global accessibility, cloud platforms face challenges like **data breaches**, **identity misuse**, **misconfigurations**, and **multi-tenancy risks**.

Traditional perimeter-based models are no longer sufficient. Modern cloud environments require **continuous verification, automation, and AI-based monitoring**. This paper summarizes emerging trends and common challenges impacting cloud security.

2. Literature Review

The literature reviewed for this study reveals multiple emerging themes in cloud security research and industry practice.

Key Themes

- **Zero Trust Security:** Focus on continuous verification of users, devices, and workloads (Kumar & Mehta, 2024).
- **AI and Machine Learning:** Intelligent systems are increasingly used to identify hidden anomalies and automate security responses (Patil et al., 2024).
- **Misconfiguration Risks:** Over half of reported breaches result from improperly configured resources (Mitchell, 2024).
- **Multi-Cloud Management:** Nearly 70% of enterprises work across multiple cloud vendors, leading to increased complexity (Thales, 2024).
- **DevSecOps Integration:** Embedding security into CI/CD pipelines helps reduce vulnerabilities early (Sharma & Gupta, 2025).
- **CNAPP Solutions:** Cloud-Native Application Protection Platforms combine several security tools into a unified framework.

Area	Author(s)	Contribution	Year
Zero Trust	Kumar & Mehta	Strengthening identity and access management through continuous verification	2024
AI-based Security	Patil et al.	Use of AI/ML for automated threat detection	2024
Misconfiguration	Mitchell	Detection of configuration errors and tools to prevent breaches	2024
DevSecOps	Sharma & Gupta	Embedding security into early development stages	2025

3. Research Methodology

This study uses a **descriptive and literature-based methodology** focusing on identifying current security trends, challenges, and technological advancements in cloud computing between 2023 and 2025.

3.1 Research Design

A qualitative research design was adopted to evaluate modern cloud security concepts. The process involved:

- Comparative study of major models such as Zero Trust, DevSecOps, CNAPP, and IAM
- Thematic grouping of cloud security threats
- Evaluation of security practices from prominent cloud providers
- Review of real-world case studies related to cloud incidents

No primary experiments or surveys were used. Instead, the study relied on credible secondary data from academic and industry sources.

3.2 Data Collection Sources

A. Academic Databases

- IEEE Xplore
- ACM Digital Library
- SpringerLink
- Peer-reviewed journals (IJICT, IJFMR, etc.)

These sources helped gather information on algorithms, architectures, and security strategies.

B. Industry Whitepapers & Reports

- Thales Cloud Security Report (2024)
- Fortinet Skills Gap Report (2025)
- Gartner Cloud Misconfiguration Analysis
- KuppingerCole CNAPP Compass Report (2025)

These provided practical insights, enterprise security statistics, and future predictions.

C. Case Studies from 2023–2025

- Accidental exposure of cloud storage buckets
- Identity and Access Management (IAM) loopholes
- Misconfigured multi-cloud environments
- Ransomware targeting cloud workloads

These cases highlight real-world challenges and recurring risk patterns.

3.3 Inclusion and Exclusion Criteria

Included:

- Publications from 2023–2025
- Research directly related to cloud security
- Industry reports with verified datasets

Excluded:

- Outdated studies unless foundational
- Papers unrelated to cloud security
- Marketing-driven/vendor-biased reports

3.4 Ethical Considerations

- All sources were properly acknowledged
- The study uses only publicly available secondary data
- No personal or sensitive information was included

3.5 Limitations

- No primary data/experiments
- Some recent breaches may not be publicly documented
- Cloud technology evolves rapidly; findings may change in the future

---

4. Results and Discussion

Key Findings

- Adoption of **Zero Trust** is increasing across public and private sectors.
- **AI/ML systems** significantly improve detection accuracy for unknown threats.
- **DevSecOps** helps eliminate security weaknesses during early development.
- **CNAPP platforms** centralize and simplify security monitoring for multi-cloud.
- **Misconfiguration errors** remain the most common cause of cloud breaches.
- A continuing gap exists in **skilled cloud security professionals**.

Discussion

Zero Trust Architecture

The Zero Trust model promotes the principle of "always verify." It minimizes insider threats and unauthorized ***and Machine*** access by enforcing strict identity checks and micro-segmentation.

AI Learning

AI-driven tools can detect unusual activities that traditional systems may miss. However, maintaining model accuracy and reducing false positives remain key challenges.

DevSecOps

By integrating security into every stage of the CI/CD pipeline, DevSecOps enables faster and more secure software releases.

Misconfiguration Challenges

Human error during cloud setup continues to be the top security concern. Automated auditing tools and CSPM platforms help reduce these risks.

Multi-Cloud Complexity

Organizations operating across multiple cloud environments need unified policies and automated compliance solutions to prevent configuration drift.

5. Conclusion and Future Scope

Cloud technology plays a critical role in digital transformation, but it introduces several security challenges such as identity misuse, misconfigurations, and multi-cloud governance issues. The study concludes that implementing Zero Trust principles, adopting DevSecOps pipelines, and using AI/ML tools can significantly improve an organization's cloud security posture.

Future advancements will likely focus on:

- AI-powered predictive threat analytics
- Wider acceptance of SASE (Secure Access Service Edge) frameworks
- Strengthening "security by design" principles
- Improving automated compliance capabilities
- Growing demand for certified cloud security professionals

Continuous improvement, proactive monitoring, and user awareness are essential for creating a safer cloud ecosystem

6.Refrences

Sr. No.	Author(s)	Title	Source	Year
1	Kumar, R., & Mehta, A.	Zero Trust Architecture in Cloud Computing	IJFMR	2024
2	Patil, S., Ali, R., & Khan, S.	Machine Learning for Cloud Security	JISEM	2024
3	Mitchell, B. S.	Identification of Cloud Misconfiguration Errors	ACM	2024
4	Thales Group	Global Cloud Security Study	Thales Report	2024
5	Sharma, P., & Gupta, N.	DevSecOps for Cloud-Native Security	IJICT	2025